**DEPARTMENT OF HOMELAND SECURITY**

**Transportation Security Administration**

**49 CFR Part 1572**

**[Docket No. TSA-2006-24191; USCG-2007-27415]**

**Transportation Worker Identity Credential (TWIC) Biometric Reader Specification and TWIC Contactless Smart Card Application**

**AGENCY:** Transportation Security Administration; United States Coast Guard; DHS.

**ACTION:** Notice of availability.

**SUMMARY:** The Department of Homeland Security, through the U.S. Coast Guard (Coast Guard) and the Transportation Security Administration (TSA), announces the availability of the working specification for Transportation Worker Identification Credential (TWIC) biometric readers and the TWIC contactless smart card application. This specification is based on recommendations to the Coast Guard and TSA from the National Maritime Security Advisory Committee (NMSAC); comments from the public following publication of the NMSAC recommendations and request for comment; and, the government's review of the NMSAC recommendations and comments received. The working specification is available to review at www.tsa.gov/twic and at http://dms.dot.gov in docket USCG-2007-27415.

**DATES:** The reader specifications and card application are available September 20, 2007.

**FOR FURTHER INFORMATION CONTACT:** John Schwartz, Office of Transportation Threat Assessment and Credentialing (TSA-19), Transportation Worker Identification Credential Program Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; telephone (571) 227-2177; facsimile (703) 603-0409; e-mail john.schwartz@dhs.gov.

Reviewing Comments and the TWIC Working Technology Specification in the Docket

Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477), or you may visit http://dms.dot.gov.

You may review the comments in the public docket by visiting the Dockets Office between 9:00 a.m. and 5:00 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located in the West Building Ground Floor, Room W12-140, at the Department of Transportation address, previously provided under ADDRESSES. Also, you may review public dockets on the Internet at http://dms.dot.gov.

**Availability of Document**

You can get an electronic copy of this Notice and the actual working specifications using the Internet by--

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (http://dms.dot.gov/search);

(2) Accessing the Government Printing Office's web page at http://www.gpoaccess.gov/fr/index.html **(Notice only)**; or

(3) Visiting TSA's Security Regulations web page at http://www.tsa.gov and accessing the link for "Research Center" at the top of the page.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this action.

## I. BACKGROUND

The National Maritime Security Advisory Council (NMSAC) was created pursuant to the Federal Advisory Committee Act, 5 U.S.C., App. 2 (FACA) in 2003. The membership of NMSAC, which includes 21 voting members, was selected to represent a broad range of viewpoints regarding maritime security challenges and to advise the Secretary of Homeland Security through the Commandant of the Coast Guard of relevant maritime security issues.

At the NMSAC meeting of November 14, 2006, the Coast Guard and TSA asked NMSAC to provide advice on a contactless biometric smart card application and reader specification for TWIC by February 28, 2007, taking into account expertise from the biometric credentialing industry and maritime/TWIC industry stakeholders. The specification is necessary for biometric readers and the TWICs that will be issued to individuals in the initial rollout of the TWIC program, beginning in the fall of 2007, and that will be used in pilot programs required by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act)[1].

TSA and Coast Guard provided NMSAC the following baseline requirements for the specification:

1. Be non-proprietary;

[1] Pub. L. 109—347; October 13, 2006.

2. Incorporate appropriate security and privacy controls;

3. Be interoperable with FIPS 201-1 credential specifications;

4. Be capable of serving as a platform for future capabilities;

5. Be capable of supporting maritime operations; and

6. Be suitable for manufacturing.

TSA and Coast Guard recommended that the task be addressed by dividing responsibilities to construct operational maritime requirements and technology specifications. We recommended that members of the maritime industry develop operational maritime requirements and address credential authentication (e.g. authentication time and process, and alternate authentication procedures) requirements; durability requirements; and credential management procedures, including key management. We recommended that the biometric credentialing experts develop technology specifications, including a smart card, reader, and keying specifications.

In the course of our discussions with NMSAC, members of the committee stated that they did not wish to recommend a specification that included encryption of the biometric and corresponding processes to decrypt the biometric when the card engages the reader. Many of the NMSAC members asserted that encryption was not necessary because the biometric – a fingerprint minutiae template, rather than an actual fingerprint – should not require the added protection that encryption provides. Also, members of NMSAC did not want to take on the additional responsibility of key management, which would be necessary if the recommended specification included encryption. However, TSA and Coast Guard disagreed with NMSAC's suggestion that the fingerprint template does not need to be encrypted and therefore asked NMSAC to provide one specification

with encryption of the biometric and a corresponding process to decrypt the biometric when the card engages the reader. The formal request from the TWIC program to NMSAC is available at the following URL: http://homeport.uscg.mil, and in the docket for this notice.

On March 1, 2007, the Coast Guard received NMSAC's report, entitled "Recommendations on Developing a Contactless Biometric Specification for the TWIC." The report included two specifications. The first recommended specification, preferred by NMSAC for the reasons discussed in the paragraph above, does not provide for encryption of the TWIC cardholder's biometric fingerprint minutiae template. Without encryption, the template is transmitted in the clear and could be read by a third party whenever the card is energized by a contactless reader. Therefore, there is a risk that the template on the TWIC could be read without the knowledge or overt action of the cardholder.

NMSAC's second specification includes encryption of the biometric fingerprint minutiae template, which will protect the template from being decrypted unless information on the card's magnetic stripe or contact integrated circuit chip (ICC), is also provided to the reader. The information on the card's magnetic strip (or ICC) is needed to decrypt the template, which is obtained contactlessly from the card. This method of encryption protects the template from being read even if it is obtained covertly since the information on the card's magnetic stripe (or ICC) cannot be obtained without physical possession of the card. If a TWIC is physically obtained by someone other than the rightful owner, the information necessary to obtain and decrypt the template would be available to them.

Note that each TWIC will contain three magnetic stripes and the first is reserved exclusively for TSA's use to store encryption information. Owner/operators may use the remaining two magnetic stripes for information that facilitates the use of local access control systems so long as doing so does not interfere with the information encoded by TSA on the first magnetic stripe that allows contactless operation of the TWIC. Technical specifications for the magnetic stripe and areas reserved for TSA use are contained in the TWIC contactless card and reader working specification.

In March 2007, the Coast Guard published a Notice of Availability of the NMSAC Recommendations and requested comments from all interested parties. (72 FR 12626, March 16, 2007.) In addition to requesting general comments, Coast Guard asked the public to respond to specific questions, including: 1) whether the use of a Personal Identification Number (PIN) is justified to further minimize the chance that a fingerprint template from a lost or stolen credential could be obtained by an unauthorized individual; 2) what, if any, privacy concerns exist if the fingerprint template is obtained by an unauthorized individual; 3) how the recommended specifications impact maritime security and operations; 4) how the recommended specifications impact existing physical access control systems (PACS); 5) whether TSA and Coast Guard should consider alternative designs; 6) how the recommended specifications impact product, system, and operational costs; 7) how quickly the recommended specifications could be incorporated into the design and manufacture of access control equipment; and 8) whether there should be a qualified products list (QPL) or equivalent regime.

Over thirty separate entities submitted comments to these questions. The majority of commenters represented the maritime industry, but several technology companies and

trade associations also responded. Generally, the commenters praised the work of the NMSAC TWIC Contactless Specification Workgroup. TSA and Coast Guard agree that NMSAC delivered excellent recommendations in a very short time-frame, and we greatly appreciate NMSAC's efforts in this important security endeavor. In the following section, we summarize all comments received.

## II. SUMMARY OF COMMENTS

Question 1 – Additional Security Features

Commenters generally agreed that the additional security feature mentioned, a PIN, was not a good idea for general use due to operational concerns. Others stated that a PIN should be considered only if it could be used in a way that does not adversely impact maritime operations. Many commenters stated that TWIC holders would likely forget their PINs, which would become burdensome to TWIC users and maritime operations. As for PIN length, the few who commented prefer a 4-digit PIN over a longer PIN.

Only one commenter discussed an alternative security feature—the use of a smart card holder that protects information stored on the card's integrated circuit chip until the holder is activated by the card holder's live biometric. At least one commenter suggested that to help deter fraudulent use of the TWIC, fingerprint scanners associated with card readers should be able to confirm that the fingerprint being presented is that of a live person rather than an artificial replica of a fingerprint or fingerprint template. This capability is called "liveness" detection.

Question 2 – Privacy Concerns

Most commenters from the maritime industry stated that maintaining the privacy of the information stored on the card is important, but they do not believe additional

measures are necessary to protect the privacy of biometric fingerprint templates. However, commenters from the technology industry generally asserted that biometric fingerprint templates should be protected, and that the TWIC Privacy Key (TPK) scheme provided in NMSAC's alternative recommended specification is sufficient to protect the template.

Question 3 – Vessel and Facility Security Operations

A number of maritime commenters stated that use of a PIN and TPK card swipe scheme, and, encryption of the fingerprint biometric template have the potential to adversely impact port and facility operations. Specifically, commenters expressed concern about error rates that might impact gate throughput, particularly during times of high-volume access; and, the effect of requiring the use of both PINs and biometrics at certain Maritime Security (MARSEC) levels. Commenters also mentioned that the upcoming TWIC pilot program that TSA and Coast Guard are implementing to test card and reader interaction will be helpful in identifying impacts on facility and vessel operations.

Question 4 – Impacts on Existing Physical Access Control Systems

Commenters generally agreed that the TWIC program will have a significant impact on existing PACS if the two are integrated and will be duplicative if they are not. They cited the need for replacing or enhancing existing systems; additional trenching and related construction activities; and, installing or upgrading electrical power supplies and wiring to readers as examples of the impacts TWIC will have on existing PACS. Some commenters mentioned that the use of TPK would impact legacy PACS by requiring the modification or replacement of existing readers to include a magnetic stripe reading

capability. Some commenters expressed concern that multiple credentials may be required of certain workers at certain locations and that multiple credentials would have to be processed to allow entry. Several commenters asserted that the cost of integration should be supported by Federal grant funding. One commenter suggested that TWIC PACS requirements should have a long phase-in period to allow facilities to use legacy equipment through the end of its useful life.

Question 5 – Alternative Designs

Commenters mentioned that any alternative designs should be evaluated in the context of the maritime operating requirements established by the NMSAC working group. Several commenters suggested that the short time period allotted for development of the technical specification may have prevented alternative designs from emerging. However, a technology industry commenter stated that alternatives were considered and rejected by the technology team during their deliberations. The commenter stated that the following alternative designs were considered and rejected:

1. Shared symmetric keys

Key management is operationally complex and exposure of the key would have a negative impact on the entire TWIC system. Shared symmetric keys rely on one secret key to be distributed among all readers and cards to establish secure communications between card and reader. Keys must be changed regularly, and securely distributed and stored to maintain system security. Secure key management would be difficult to accomplish due to the number and dispersion of TWIC readers.

2. Public Key Infrastructure (PKI)

In a PKI system, secure communication and authentication are done using public key certificates which require online communication. The fragmented TWIC PACS would lack the real-time network access required of a PKI system.

3. Biometric Match-on-Card (MOC)

MOC involves matching a biometric sample against a reference biometric template stored inside the secure environment of a smart card. The reference template cannot be read outside of the card, but is only used internally by the matching process inside the smart card. MOC is a relatively new approach within the smart card and biometrics industries and provides a good level of security and privacy. This is because the user's biometric information is protected by the smart card and is never released from the card. Internal to the smart card, MOC matches the user's live biometric template provided by an external biometric reader with the user's stored reference template. A major advantage to MOC over other approaches is that the card never releases personally identifying information (the biometric template) to the reader. Thus, the biometric could not be lifted or 'skimmed' by an unauthorized individual. Also, under the MOC process, the need for reader authentication and associated reader key management is minimized because the reader only stores public keys that do not need to be protected from disclosure by using a Secure Access Module (SAM) to store secret keys to identify a particular smart card. With MOC, the transmission of the biometric template from the reader to the card is done using the public key and can only be decrypted using the private key that is stored securely on the smart card. For all of these reasons, MOC is a very promising technology to pursue. However, it has not been fully tested in a variety of laboratory or field settings and currently, there are no approved MOC standards.

Therefore, we have determined that it would not be advisable to implement MOC for the upcoming TWIC rollout. We will continue to follow the development of MOC and if it matures for operational use, we will again consider its use in the maritime environment.

One commenter requested that the distance between the card reader and the card be increased from four to 18 inches to allow truck drivers to remain in their cabs while their TWICs are read. Some commenters reiterated their view that the specification should not include encryption in any form.

Question 6 – Cost Impacts

A number of commenters reiterated their endorsement of NMSAC's non-encryption recommendation to minimize costs. Commenters who operate existing PACS expressed concern about integrating TWIC into their operation, particularly if encryption of the biometric is required and if wiring upgrades are necessary to support TWIC readers. Commenters who do not have PACS now expressed concern about how much it will cost to purchase, install, and maintain TWIC systems.

Question 7 – Incorporation of TWIC into Existing Access Control Equipment

Maritime industry commenters generally deferred this question to the technical experts. Technical commenters stated that the specifications TSA and Coast Guard choose for the TWIC program will determine the ease of design, manufacture, and integration. They also stated that knowledge gained through experience with designs for other PACS that share common attributes with TWIC will lessen the time needed to create TWIC PACS products. Conversely, features that are unique to TWIC will have to be created, but some commenters believe TWIC-unique features can be accommodated through software or firmware (i.e. computer programming instructions that are stored in a

read-only memory unit rather than being implemented through software) applications for existing readers. The commenters estimate that it may take from only a few months up to 36 months to integrate TWIC with certain PACS designs.

Question 8 – Quality Products List Process & Creation

Almost universally, commenters agreed that TSA and Coast Guard should use a QPL process to help stakeholders know what equipment is best for use in the maritime environment. Many commented that the process the U.S. General Services Administration uses should be considered as a starting point for development of a TWIC QPL. Commenters also stated that product testing should include harsh maritime conditions.

## III. WORKING SPECIFICATION SELECTED

### A. Summary of Selection

TSA and the Coast Guard have selected the NMSAC alternate recommendation that requires encryption and use of the TWIC Privacy Key (TPK) as the working specification for readers that will be used during the pilot programs. If the readers that meet this working specification perform as planned during the pilot testing, we will finalize the specification as we complete the rulemaking that requires the use of readers. Also, it is important to note that the TWICs that will be issued this fall in the initial rollout of the TWIC program will operate as designed when engaged in readers that are built to this working specification.

We are choosing to adopt this specification to protect the personally identifiable information (PII) contained in the TWIC from unintended disclosure while the TWIC is in the possession of the credential's rightful owner. Even assuming individuals suffer no

real injury today if their template is taken or lifted through an unauthorized process, the template is personal information connected to that individual. Using a fingerprint template in lieu of a fingerprint image does not necessarily prevent the long-term potential for unauthorized use of personally identifying fingerprint information, if intercepted by unauthorized persons. Even assuming the fingerprint template cannot be reverse-engineered to produce an accurate duplicate fingerprint today, we cannot be certain that such a capability will not arise in the future. With the use of the TPK model, security and privacy protection are provided without the burden that other encryption models would place on PACS owners and operators.

TSA and Coast Guard take the industry's concerns about adverse operational impacts very seriously. Consequently, as the card and readers are envisioned to operate when TWIC is fully implemented, use of a PIN will not be necessary to release the biometric unless the owner/operator chooses to use contact readers and the contact side of the credential. In addition, we are in the process of finalizing plans for the pilot tests required by the SAFE Port Act and we are working with experts within DHS to establish a very thorough test plan to evaluate the card-reader interface under a variety of conditions and assess its impact on operations. Through the pilot tests, we will investigate the impacts of requiring biometric identity verification on business processes, technology, and operations on facilities and vessels of various size, type, and location. As detailed below, while the government has removed any specific language about MARSEC levels from the specifications, the pilot testing process will be used to evaluate various use case scenarios that will influence the upcoming TWIC reader rulemaking process, including TWIC card and reader use requirements at various MARSEC levels.

We understand that the decision to implement the TPK model for contactless biometric identity verification will have impacts on the installed base of PACS systems. However, the TPK model allows facilities to integrate the model with their local PACS in several different ways. The TPK model allows use of: (1) the magnetic stripe to transfer TPK information by swiping the card through a magnetic strip reader and then presenting the card to a contactless reader to securely transmit the biometric template; (2) pre-registration of the information on the magnetic stripe into the local PACS and then presenting the card to a contactless reader; or, (3) pre-registering the biometric minutiae templates into the local PACS until retrieved upon presentation of the TWIC to a contactless reader. The TPK model also allows several options for handheld readers. Handheld reader options include the use of either the contact or contactless portion of the TWIC to enable biometric identity verification.

We do not wish to implement any alternative designs at this time. However, we may add additional security features to the card or card reader with due notice to the industry and regard for operational impacts. One alternative technology of particular interest to the government is match-on-card (MOC) technology. The TWIC program and Coast Guard remain in close contact with the National Institute of Standards and Technology (NIST) in their consideration of MOC technology for various Federal smart card and personal identification initiatives.

We are mindful that cost is a strong consideration in the operational implementation of TWIC and we are working to minimize costs on the operational users of TWIC where possible. Also, we are working closely with other DHS components to

continue to make available Port Security Grant funds to mitigate some of the costs to vessel and facility operators and owners of implementing the TWIC program.

We have worked closely with the NMSAC working group to understand the impacts of the TWIC program on the maritime sector. Our choice of the TPK model is grounded in the specific recommendation of smart card, PACS, and biometrics industry experts involved in the NMSAC working group process and a thorough review of technology choices and impacts by government experts. These experts leveraged other similar technologies from contactless identification regimes in their deliberations. While implementation of the TWIC program should be as timely as possible, we understand that technical implementation timelines must incorporate engineering and manufacturing time, field testing, facility adaptation, and final field installation.

We are encouraged by the positive responses we received regarding the creation of a QPL. However, unlike other government smart card programs, TWIC card readers, in most cases, will not be procured by the government. This lessens the ability of the government to leverage existing QPL-type programs already in existence such as those supporting the Homeland Security Presidential Directive (HSPD)-12 Personal Identity Verification (PIV) Program.

B. Technical Changes to the TPK Working Specification

TSA and Coast Guard are making some technical modifications to the TPK working specification recommended by NMSAC. We believe these changes are necessary to further protect privacy and security for the TWIC program. There are four important changes involving verification of the cardholder unique identifier (CHUID) data, MARSEC level operations, biometric liveness detection, and contactless

transmission speed that are discussed in detail below. In addition, we made minor changes to the specification that is discussed below.

B.1. Signature Verification of CHUID Data

The NMSAC specification recommends that verification of the signature on the CHUID be optional. However, regardless of whether the credential is digitally signed, CHUID data can be copied or "cloned" to another card. Signature verification mitigates counterfeited CHUID data from being accepted as authentic. For this reason, verification of the digital signature on any CHUID unknown to a PACS is mandatory and is included in the final specification. Signature verification will have minimal performance impact to the contactless transaction and minimal impact on reader implementation.

B.2. Authentication Methods Used at MARSEC Levels

NMSAC recommended that CHUID authentication should be used at MARSEC 1 and biometric authentication should be used at MARSEC 2. Specifying authentication methods for various threat or risk levels is outside of the scope of a technical specification for contactless cards and readers, and is more appropriately addressed separately in the risk management and security requirements for maritime operators. Therefore, we have removed the MARSEC guidance relating to use of specific authentication levels at different MARSEC levels from the working specification.

B.3. Biometric Liveness Detection

NMSAC recommended that biometric liveness detection may be employed in TWIC readers, making liveness detection optional. Liveness detection is an important means to prevent spoofing of a biometric sensor and is generally something that is strongly recommended by the reader industry. Because standards for liveness detection

are currently not available, and there is no conformance testing protocol to validate its effectiveness, it is difficult to specify liveness detection as a mandatory requirement. However, we have changed the language for liveness detection from may to should, to stress that liveness detection (or attended verification) in TWIC readers is a highly desirable feature. This change will have no operational impact on TWIC contactless transactions.

B.4. Contactless Transmission Speed

The contactless reader performance requirements in the NMSAC specification are based upon transaction completion time. We have determined that specific requirements for contactless transmission speed should be specified so that the reader will support negotiation of a contactless speed with the card that achieves at least 400K bits per second. This will minimize transaction timings based on transmission capabilities of both current and future TWIC card versions. This change will not adversely impact TWIC contactless transactions.

C. List of All Changes to the TPK Specification

Listed below is a complete list of the changes TSA and Coast Guard have made to the TPK specification that NMSAC recommended. The changes of interest are discussed in detail above in Section III.B.

1. Section 4, TWIC Modes of Operation. Requirement for specific authentication modes to be used at specific MARSEC levels has been removed and available authentication modes have been clarified.

2. Section 4, TWIC Modes of Operation. Ability to configure specific authentication modes depending on a given perimeter security requirement and to be used at differing MARSEC levels has been added.

3. Section 4, TWIC Modes of Operation. Verification of CHUID signature changed to mandatory. CHUID signature is either verified once, either when the card holder's CHUID is registered in a local PACS, or read by the TWIC reader each time the card is presented for access.

4. Section 5.1.1, Device Dimensions. Note added to stress contactless reader sensitivity to location and electromagnetic conditions of their environment.

5. Section 6, Portable Reader Requirements. Requirements for confidentiality and authentication added for wireless devices used in physical access systems.

6. Section 7, Operational Requirements. Contactless transmission speed requirement changed to support 106kbit/s, 212kbit/s or 424kbit/s, based on the card's capabilities.

7. Section 7, Operational Requirements. Requirement added to reject transaction if multiple cards are simultaneously detected in the reader's contactless field.

8. Section 8, Performance Requirements. Support for biometric liveness detection strengthened from "may" to "should" indicating a strong preference for liveness detection.

9. Appendix A.1, CHUID Authentication. CHUID authentication clarified.

10. Appendix A.2, TWIC Biometric Authentication. Biometric authentication clarified.

11. Appendix A.3, Card Authentication Key Authentication. Card Authentication data object reference corrected.

12. Appendix A.3, Card Authentication Key Authentication. Card Authentication Key usage clarified to indicate that it is only available via the PIV application, and is not shared with the TWIC application.

13. Appendix D, TWIC Reader Compatibility with Other Card Types. Reader compatibility and default card support clarified and modified to allow configuration of default AID.

14. Appendix E.4, Alternate Implementations. Minor clarifications to PACS enrollment.

15. Appendix F, Proposed TWIC AID Structure. TSA RID added, AID structure clarified.

D. Future Changes to Specification

TSA and Coast Guard will continue to evaluate and test the working specification as we implement the TWIC Pilot Program. We anticipate that, as with any testing program, we will encounter technical issues that can be corrected by making minor changes to the working specification. We will make such changes available to the public as they occur, through use of the following link/website: www.tsa.gov/twic. In addition, we will address any necessary changes to the working specification prior to finalizing the regulations requiring TWIC readers. .

Issued in Arlington, Virginia, on SEP 14 2007

Stephanie Rowe,

Assistant Administrator,

Transportation Threat Assessment and Credentialing,

Transportation Security Administration.